SD-WAN for NGFW

SD-WAN Subscription for NGFWs

SD-WAN for NGFW allows you to easily adopt an end-to-end SD-WAN architecture with natively integrated, world-class security and connectivity.

The effects of the cloud on network and security transformation are undeniable. As the number of devices at branch locations grows and applications become more bandwidth-intensive, businesses are forced to spend more to accommodate demand. As a result, traditional wide area network (WAN) architectures with multiprotocol label switching (MPLS), which tend to eat up bandwidth as they backhaul traffic from branches to the cloud, render legacy approaches ineffective.

Benefits

- Deliver consistent, integrated security across branch, data center, and cloud by leveraging the industry's leading ML-powered NGFW to protect applications, users, and devices against all threats.
- Optimize your performance by gaining the flexibility to leverage Prisma Access hubs, data center hubs, or branches for application access.
- Simplify branch onboarding using Prisma Access hubs and data centers as the global backbone while centrally managing security and networking policies.

Software-defined wide area networking (SD-WAN), an approach that uses commodity links and allows you to intelligently manage as well as control connectivity between branches and cloud instances, is now a necessity for distributed enterprises. According to Gartner, by 2023, more than 90% of WAN edge infrastructure refreshes will be based on vCPE platforms or SD-WAN vs. traditional routers.[1] However, with its benefits, SD-WAN also brings many challenges, such as a lack of security, unreliable performance, and complexity.

When security is an afterthought, it tends to be either subpar or bolted on, introducing management complexity. Moreover, network performance becomes less reliable because enterprises use the congested internet as the WAN middle mile—and when they try to address this by building their own SD-WAN hub infrastructures, they run into complexity. Ultimately, enterprises turn to multiple vendors or service providers to solve performance issues, which increases costs while decreasing control and visibility.

SD-WAN for NGFW by Palo Alto Networks

SD-WAN for NGFW from Palo Alto Networks lets you easily adopt an end-to-end SD-WAN architecture with natively integrated, world-class security and connectivity. Using hub-and-spoke and/or full-mesh branch-to-branch topologies, you can optimize the performance of your entire network. This minimizes latency and ensures reliability, resulting in an exceptional user experience at the branches. Each site automatically creates a meshed VPN connection to all other sites to load balance sessions, failover to a better-performing link, and take advantage of all available bandwidth to maximize throughput capacity. Regardless of your deployment model, our tight integration will allow you to manage security and SD-WAN on a single, intuitive interface.

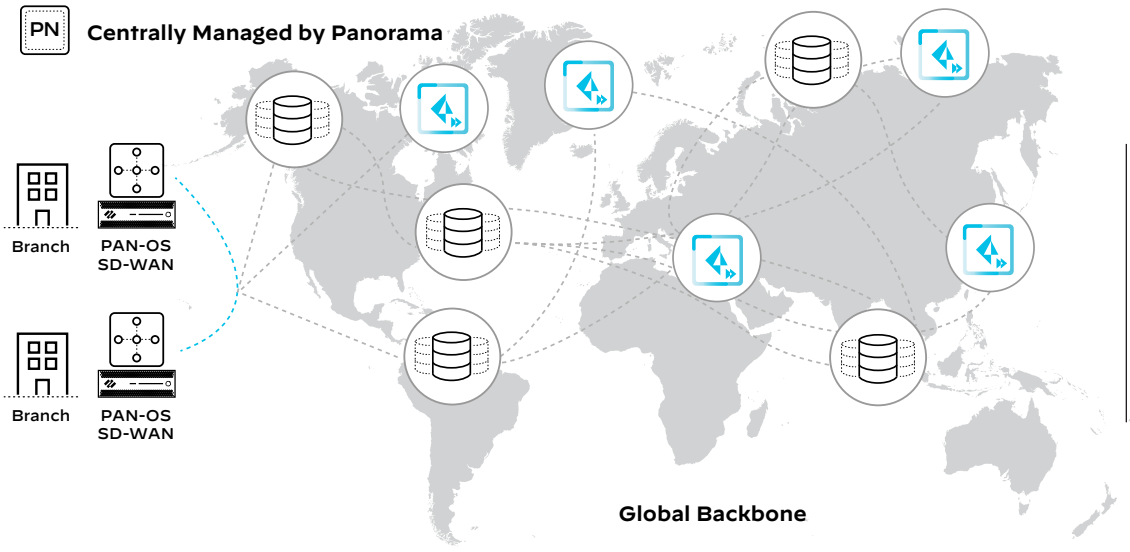
Optimized Connectivity for Improved User Experience

PAN-OS SD-WAN lets you measure and monitor specific paths as well as dynamically move sessions to the optimal path, guaranteeing the best branch user experience. You can simply enable the subscription on your next-generation firewalls and begin intelligently and securely routing branch traffic to your cloud applications and between other sites. Through a concept called "link bundling," the firewall will automatically combine all service provider links labeled with the same link tag to aggregate bandwidth and distribute traffic between them, maximizing all available capacity.

Complete Application Control

SD-WAN for NGFW gives you full control of when to select a better path for your applications. Using profiles for path health quality, software-as-a-service (SaaS) application path monitoring, error correction (forward error correction and packet duplication), and traffic distribution, each application can have its own set of thresholds and path forwarding rules. With DIA AnyPath, you can tailor exactly how an internet application fails over—either to another DIA internet path at the same site or through a private VPN path to another location to get better internet service. This ensures that all mission-critical applications are performing at their best to provide the highest level of usability.

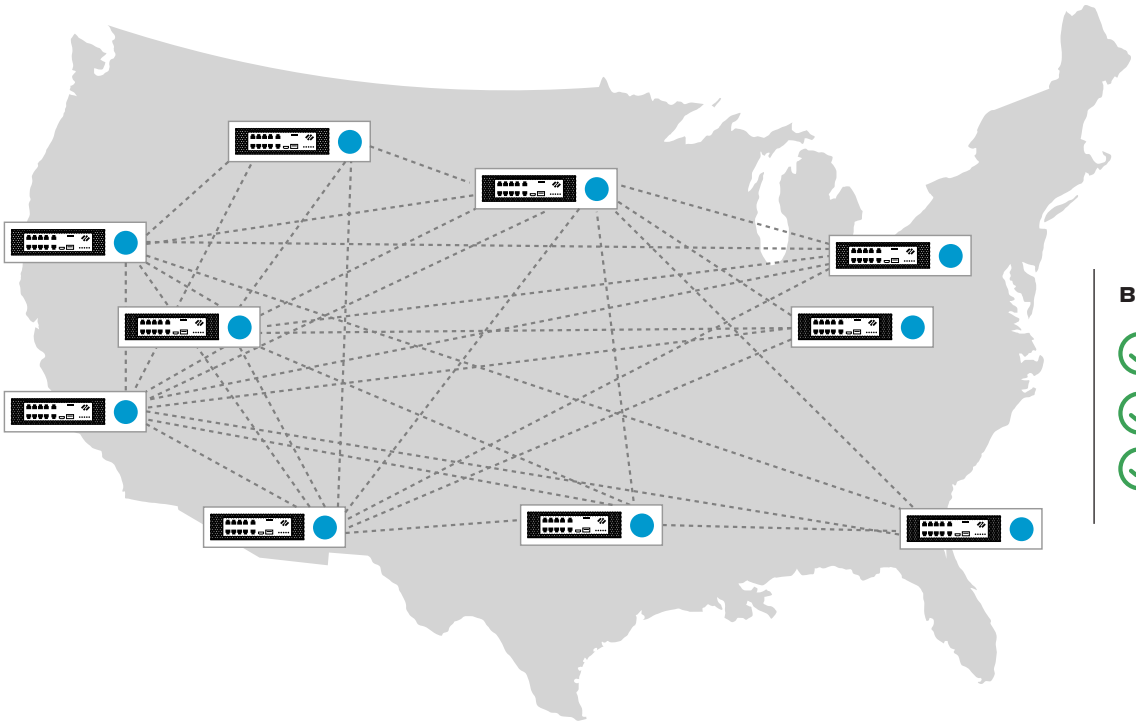
1. *Gartner® Magic Quadrant™ for WAN Edge Infrastructure*, Gartner, October 18, 2018, https://www.gartner.com/en/documents/3891709.



Benefits

- Expedite cloud on-ramp
- Best security with zero upgrades
- Faster middle-mile cloud connections

Figure 1: SD-WAN for NGFW for Global Interconnect



Benefits

- Direct connectivity between branches
- No hub required
- Ideal for small-scale, regional deployments

Figure 2: SD-WAN for NGFW mesh approach

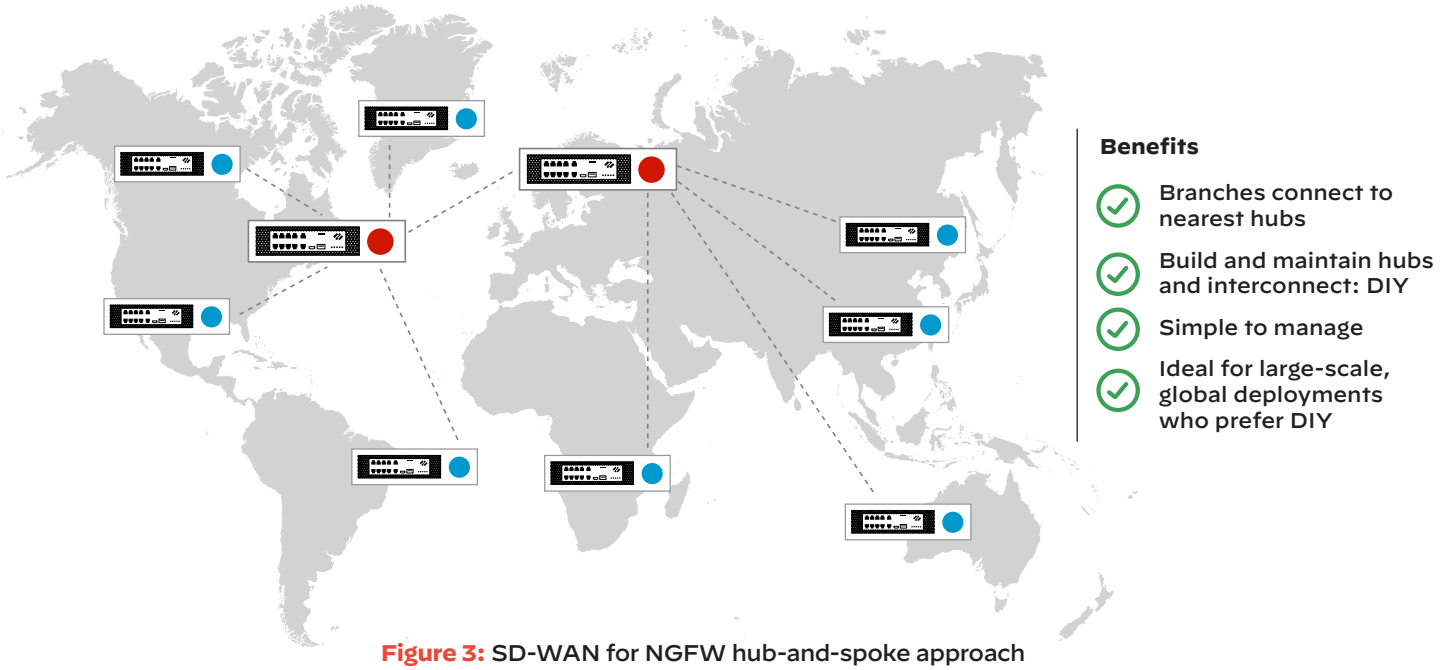


Figure 3: SD-WAN for NGFW hub-and-spoke approach

Central Management for Security and Connectivity

Eliminate the need to manage multiple disparate consoles from different vendors by using Panorama network security management for both security and connectivity. Integrated SD-WAN configuration and monitoring allow you to leverage the familiar Panorama user and application workflow, cutting the time you need to spend reconfiguring policies and visualizations. Additionally, you get granular SD-WAN monitoring data and a dedicated configuration tree, giving you greater visibility into your network.

Simplified Branch Onboarding

Provisioning a new branch requires IT staff to configure and deploy appliances. Doing this on a large scale and at distributed locations makes branch onboarding costly and slow. With Zero Touch Provisioning (ZTP), you can automate tedious onboarding processes. Appliances can be drop shipped to your branch locations, where they are powered up and connected to the internet. To complete onboarding, administrators simply need to register on a web portal. Then, they can immediately start managing deployment and configuration from a single location through Panorama.

Flexible Deployment Options

Palo Alto Networks supports multiple SD-WAN deployment options, including mesh, hub-and-spoke, and cloud-based deployments. SD-WAN for NGFW is supported on all PA-Series (hardware) and VM-Series (virtual) NGFW platforms.

SD-WAN Software Licenses

(Required) SD-WAN for NGFW subscription on all PA-Series and VM-Series firewalls (VM-50 and above). This license requires PAN-OS 9.1 and above.

Table 1: Palo Alto Networks SD-WAN-Supported Features and Capabilities	
Category	**Features**
AAA/Authentication	RADIUS, local authentication and authorization, multitenant three-tier RBAC architecture, auditing, roles, and privileges
Availability	Hardware high availability in active/passive mode
SD-WAN Features	· Link metric collection, jitter, drop, delay · Intelligent path selection based on metric; dynamic application steering · Application and network condition-aware sub-second steering · Session-based link aggregation · Scalable bidirectional path health measurements, QoS, traffic shaping · Predefined application thresholds for common application categories · Forward error correction (FEC) · Packet duplication · SaaS application path monitoring: end-to-end application monitoring from the branch to the SaaS app server · DIA AnyPath: failover DIA internet applications to any other link (DIA, VPN, or MPLS) · Single and double NAT support · DDNS support · Priority-based hub failover · Per-application split tunneling
Network Services	IPv4, DNS, DHCP client, DHCP server, DHCP relay, NAT
Dynamic QoS/Traffic Shaping	· QoS shaping, policing, and rate limiting with per-flow queueing and separate cleartext and tunnel treatment · Support for eight queues, type of service (ToS), and DSCP code points with patented bidirectional session-based DSCP tagging
Routing	· Static routes · OSPF · BGP » Local route ID and local AS, path selection, BGP confederations, route flap dampening, graceful restart, IGP-BGP route injection » Route import, export, and advertisement; prefix-based filtering; address aggregation · Multiple virtual routers · Authentication by MD5
SD-WAN High Availability	Active/Passive HA; dual power supply
Connectivity Architecture	· Hub-and-spoke IPsec tunnels with automatic configuration · Full mesh · Prisma Access Hub support
Management	· Single pane of glass for security and SD-WAN management · Panorama-managed, API, syslog, SNMP · RBAC · Scale up to 5,000 devices per Panorama · Zero Touch Provisioning (ZTP) · Monitoring and visualization · Dashboard views of SD-WAN-impacted applications and links with drill down · SD-WAN link down alerts to detect blackout situations · SD-WAN reporting · Link jitter, delay, and drop trend charts
Deployment Flexibility	· Physical and Virtual Next-Generation Firewalls for both branch and hub · Hub and spoke · Full mesh · Cloud-delivered with Prisma Access hubs

Table 2: SD-WAN Device Specifications (Hardware)*†									
	PA-400 Series	PA-800 Series	PA-1400 Series	PA-3200 Series	PA-3400 Series	PA-5200 Series	PA-5400 Series	PA-5450	PA-7000 Series
Branch Office Bandwidth (recommended range)	200 Mbps–1.25 Gbps	50–700 Mbps	2.5–4 Gbps	800 Mbps–3 Gbps	5–10 Gbps	—	21–58 Gbps	—	—
Max. Overlay IPsec Tunnels	1K–2.8K	1K	2.8K	2K–3K	5K–8K	3K–5K	24K	24K	8–12K
IPsec Overlay Performance with App-ID	900 Mbps –1.5 Gbps	1 Gbps	4–6.5 Gbps	2–3.5 Gbps	6.5–14 Gbps	7–22.5 Gbps	20–80 Gbps	TBD	22–300 Gbps
Max. Concurrent Sessions	64K–400K	128K–196K	945K–1.4M	1M–3M	1.4M–3M	4M–64M	3.2M–100M	3.2M–200M	19.2M–80M
Max. Number of Routes	2.5K–10K	5K–10K	10K	16K–44K	10K–24K	100K	228K	228K	32K–64K
Connectivity Options									
LAN/WAN 1G RJ-45	7–8	4	8	—	12	—	Depends on cards	Depends on cards	Depends on cards
LAN/WAN 1G SFP	—	8	6	—	—	—	Depends on cards	Depends on cards	Depends on cards
LAN/WAN 1G/10G SFP	—	4	4	8	10	16	Depends on cards	Depends on cards	Depends on cards
LAN/WAN 40G QSFP	—	—	—	0–4	2 PA-3430 PA-3440	4	Depends on cards	Depends on cards	Depends on cards
HA—Dual Power Input	Optional	Yes (PA-850)	Optional	Optional	Yes	Yes	Yes	Yes	Yes
Appliance Datasheet	Learn more	Learn more		Learn more		Learn more	Learn more	Learn more	Learn more

* Any appliance can be used as a hub or branch.

† Ranges shown represent the span of appliance SKUs in a given series.

Table 3: SD-WAN Device Specifications (Virtual Machines)*					
	VM-50	VM-100	VM-300	VM-500	VM-700
Branch Office Bandwidth (recommended range)	1–250 Mbps	200–450 Mbps	400 Mbps–1 Gbps	—	—
IPsec Overlay Performance with App-ID	945 Mbps	967 Mbps	1.6 Gbps	3.5 Gbps	6.9 Gbps
Max. Overlay IPsec Tunnels	250	1K	2K	4K	8K
Max. Concurrent Sessions	64K	256K	819K	2M	10M
Max. Number of Routes	2.5K	5K	10K	32K	100K
Appliance Datasheet	Learn more				

* Any appliance can be used as a hub or branch.

To compare performance and specifications for all our firewall offerings, visit paloaltonetworks.com/products/product-selection.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com